AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A process that monitors network traffic through a monitoring device disposed between a data center and a network for thwarting denial of service attacks on the data center, the process comprises:

a detection process to determine if the values of a parameter of network traffic exceed normal values for the parameter to indicate an attack on the data center;

a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack; and

a filtering process for filtering of network packets based on the characterization ~~process~~ process, wherein the filtering process comprises:

constructing a master correlation bit vector, wherein bits of the master correlation bit vector correspond to parameter correlations;

initializing bits of a packet's correlation bit vector as not suspicious;

retrieving a parameter from a parameter suspicious correlation bit vector, which comprises a list of suspicious values for the parameter, to construct the packet's correlation bit vector; and

using a value of the packet's correlation bit vector to index the master correlation bit vector.

2. (Previously Presented) The process of claim 1 wherein, in the characterization process, suspicious parameter values are represented by a bit

vector with a 1 in every position corresponding to a "bad" value, and a 0 in every position corresponding to a "good" value.

3. (Previously Presented) The process of claim 1 wherein the characterization process comprises:

a correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that indicate types of attacks.

4. (Original) The process of claim 3 wherein the correlation process is used to reduce dropping of legitimate traffic.

5. (Currently amended) The process of claim ~~2~~ 1 wherein filtering is aggregate filtering.

6. (Original) The process of claim 1 wherein parameters include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

7. (Currently Amended) A method for thwarting denial of service attacks on a data center, the method comprising:

producing a histogram of received network traffic for at least one parameter of network packets; ~~and~~

characterizing an attack based on comparison of a historical histogram with the produced histogram data for one or more ~~parameters~~ parameters; and

filtering out traffic characterized as part of an attack, wherein filtering out the traffic comprises:

constructing a master correlation bit vector, wherein bits of the master correlation bit vector correspond to parameter correlations;

initializing bits of a packet's correlation bit vector as not suspicious;

retrieving a parameter from a parameter suspicious correlation bit vector, which comprises a list of suspicious values for the parameter, to construct the packet's correlation bit vector; and

using a value of the packet's correlation bit vector to index the master correlation bit vector.

8. (Currently Amended) The method of claim 7 further comprising:

filtering network packets sent to the data center based on whether ~~or not~~ a value of ~~the attribute~~an attribute represented in the ~~current~~ produced histogram is within a normal range of ~~values~~ the values for the attribute, as determined by comparison to the historical histogram.

9. (Currently amended) The method of claim 7 wherein the historical histogram is based on time periods ~~that can range from 1 hour to 1 week or more.~~of at least one hour.

10. (Currently amended) The method of claim 7 wherein the produced histogram is produced during an attack and over time periods of ~~about~~ approximately 10-300 ~~sec or so.~~seconds.

11. (Previously Presented) The method of claim 7 further comprising:

normalizing the produced and the historical histograms for each parameter; and

computing their difference to identify significant outliers that are considered indicators of suspicious traffic.

12. (Original) The method of claim 11 further comprising:

correlating suspicious parameters to reduce blocking of legitimate traffic.

13. (Currently Amended) The method of claim 12 wherein the packet's correlation bit vector contains sufficient bits to represent the ~~whole~~ parameter space.

14. (Currently amended) The method of claim 11 further comprising:

correlating suspicious parameters to determine ~~existence of correlations of~~a correlation of those parameters that can ~~point to indications of attacks.~~indicate an attack.

15. (Currently Amended) The method of ~~claim 11~~claim 8 wherein filtering the network packets ~~based on attribute~~ further comprises:

producing ~~a master~~the master correlation ~~vector~~ bit vector from a stream of sampled packets and examining the network packets using a process that is constant-time, independently of the number of correlations or of the number of suspicious values for a parameter.

16. (Canceled).

17. (Currently amended) The method of ~~claim 16~~claim 15 wherein filtering the network packets ~~based on attribute~~ further comprises:

~~testing the bit~~testing bits in the master correlation ~~vector~~ bit vector to decide whether to drop or forward the packet.

18. (Currently Amended) The method of ~~claim 7~~claim 8 wherein ~~attributes include~~the attribute comprises at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

19. (Original) The method of claim 7 wherein the method is executed on a data collector.

20. (Original) The method of claim 7 wherein the method is executed on a gateway.

21. (Currently Amended) A monitoring device for thwarting denial of service attacks on a data center, the monitoring device comprises:

a computing device executing:

a process to build at least one histogram for at least one parameter of network ~~traffic; and~~ traffic;

a process to characterize an attack based on a comparison of a historical histogram of the at least one parameter to the built at least one histogram for the at least one ~~parameter.~~parameter; and

a process to filter network packets based on characterization, wherein the process to filter the network packets comprises:

constructing a master correlation bit vector, wherein bits of the master correlation bit vector correspond to parameter correlations;

initializing bits of a packet's correlation bit vector as not suspicious;

retrieving a parameter from a parameter suspicious correlation bit vector, which comprises a list of suspicious values for the parameter, to construct the packet's correlation bit vector; and

using a value of the packet's correlation bit vector to index the master correlation bit vector.

22. (Original) The monitoring device of claim 21 further comprising:

a process to correlate suspicious parameters to reduce blocking of legitimate traffic.

23. (Original) The monitoring device of claim 21 wherein the characterization process normalizes the historical and built histograms for each parameter and computes their difference to identify significant outliers that are considered indicators of suspicious traffic.

24. (Currently Amended) The monitoring device of claim 23 wherein the characterization process produces ~~a master~~the master correlation vector from a stream of sampled packets and examines the sampled packets using a process that is constant-time, independently of the number of correlations or of the number of suspicious values for a parameter.

25. (Original) The monitoring device of claim 21 wherein the device is a gateway device that is adaptable to dynamically install filters on nearby routers.

26. (Original) The monitoring device of claim 21 wherein the device is a data collector.

27. (Original)The monitoring device of claim 21 wherein the parameters include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

28. (Currently Amended) A computer program product residing on a computer readable medium comprising instructions for causing a processor to:

build a histogram for a parameter of network ~~traffic; and~~traffic;

use the histogram data for the parameter to characterize an ~~attack.~~attack; and

filter the network traffic based on characterization of the attack, wherein the instructions to filter the network traffic comprises instructions to:

construct a master correlation bit vector, wherein bits of the master correlation bit vector correspond to parameter correlations;

initialize bits of a packet's correlation bit vector as not suspicious;

retrieve a parameter from a parameter suspicious correlation bit vector, which comprises a list of suspicious values for the parameter, to construct the packet's correlation bit vector; and

use a value of the packet's correlation bit vector to index the master correlation bit vector.

29. (Canceled).

30. (Currently amended) The computer program product of claim 28 further comprising instructions to:

determine if ~~the values of a parameter exceed~~a parameter value exceeds a normal ~~values~~ value for the parameter to indicate an attack on the site.

31. (Currently amended) The computer program product of claim 30 further comprising instructions to:

use the histogram to characterize the attack when it is determined that ~~one of the parameters~~a parameter value exceeds a threshold.

32. (Currently Amended) A method of protecting a data center during a denial of service attack, the method comprises:

monitoring network traffic through a gateway disposed between the data center and a network:

determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site;

producing a histogram for the at least one parameter of network traffic to characterize the attack by comparing the histogram to at least one historical histogram for that parameter; and

filtering out traffic based on characterizing the traffic, which the gateway deems to be part of an ~~attack.~~attack, wherein filtering out the traffic comprises:

constructing a master correlation bit vector, wherein bits of the master correlation bit vector correspond to parameter correlations;

initializing bits of a packet's correlation bit vector as not suspicious;

retrieving a parameter from a parameter suspicious correlation bit vector, which comprises a list of suspicious values for the parameters, to construct the packet's correlation bit vector; and

using a value of the packet's correlation bit vector to index the master correlation bit vector.

33. (Original) The method of claim 32 further comprising:

communicating statistics collected in the gateway to a control center.

34. (Original) The method of claim 33 wherein communicating occurs over a dedicated link to the control center via a hardened network.

35. (Original) The method of claim 33 wherein the gateway is physically deployed in line in the network.

36. (Original) The method of claim 33 wherein filtering occurs on nearby routers.

37. (Original) A method to reduce blocking of legitimate traffic in a process to protect a victim site during a denial of service attack, comprises:

producing a histogram of network traffic to characterize an attack; and

filtering out traffic deemed part of an attack with filtering comprising:

constructing a master correlation vector having asserted bits corresponding to the most important parameter correlations;

initializing a packet's correlation bit vector to 0, and for every parameter:

retrieving the parameter in a parameter suspicious vector to construct the packet' correlation bit vector; and

using the value of the packet's correlation bit vector to index into the master correlation bit vector.

38. (Original) The method of claim 37 further comprising:

testing the indexed bit in the master correlation vector, where if the bit in the master correlation bit vector is a one, the packet is dropped, otherwise the packet is forwarded.

39. (Original) The method of claim 37 wherein the master correlation vector is constructed from a stream of sampled packets.

40. (Original) The method of claim 37 further comprising:

maintaining a correlation bit vector with as many bits as there are parameters; and

if a parameter's suspicious vector has a 1 in a bit position corresponding to the parameter's value in a packet, the method further comprises:

setting the bit corresponding to the parameter in the packet's correlation vector to 1.